(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号

特開平6－103076

(43)公開日　平成６年(1994)４月15日

(51)Int.Cl.[5]		識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ	9/445				
	1/00	３７０　Ｅ	7165－5B		
	9/06	４５０　Ｅ	9367－5B		
	15/00	３３０　Ａ	7459－5L		
			9367－5B	Ｇ０６Ｆ　9/06　４２０　Ｌ	

審査請求　有　　請求項の数５(全 13 頁)

(21)出願番号　－　特願平5－114396

(22)出願日　平成５年(1993)５月17日

(31)優先権主張番号　８８９３２４

(32)優先日　1992年５月27日

(33)優先権主張国　米国（ＵＳ）

特許法第65条の２第２項第４号の規定により×印の部分は不掲載とする。

(71)出願人　390009531

インターナショナル・ビジネス・マシーンズ・コーポレイション

INTERNATIONAL BUSINESS MASCHINES CORPORATION

アメリカ合衆国10504、ニューヨーク州　アーモンク　（番地なし）

(72)発明者　ジョン・ワイリー・ブラックリッジ・ジュニア

アメリカ合衆国33487　フロリダ州ボカ・レイトン、セコイア・レイン　304

(74)代理人　弁理士　頓宮　孝一　（外４名）

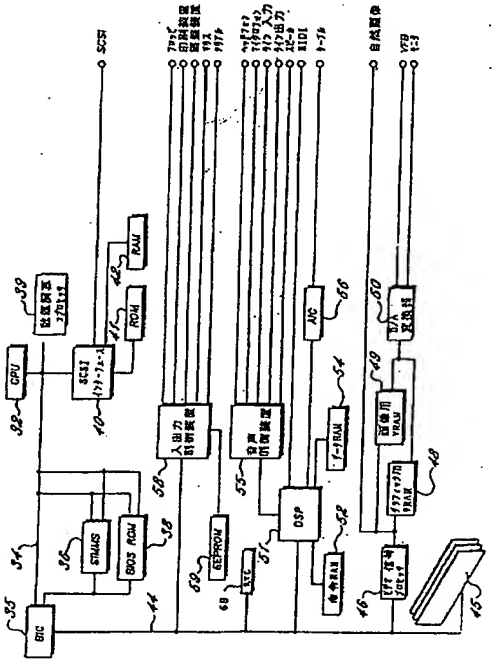
最終頁に続く

(54)【発明の名称】　セキュリティ機構を備えたコンピュータ・システム及び該機構の管理方法

(57)【要約】

【目的】　本発明の目的は、パーソナル・コンピュータ・システムに保存されているデータへのアクセスにおける制御を可能にするセキュリティ機構を提供すること。

【構成】　特定のユーザが、（ａ）複数のソースの番号と優先順序を特定することによって、初期ローディング・プログラムを選択的に変更できるための、及び（ｂ）複数のソースからインタプリタ・プログラムを削除することによって、初期ローディング・プログラムを選択的に変更できるための、セキュリティ・ユーティリティ・プログラムと、システムＣＰＵによって処理されるデータを暗号化する場合及び非暗号化する場合に使用するためのマスター暗号鍵と、特定のユーザがマスター暗号鍵を変更できるための、第２のセキュリティ・ユーティリティ・プログラムを有すパーソナル・コンピュータ・システム。



1

【特許請求の範囲】

【請求項１】データを受信・保存し、不当なアクセスに対して、該データの安全保護を図るコンピュータ・システムであって、

ユーザが命令を入力するためのユーザ入力装置と、

通常は閉じられている格納装置と、

前記ユーザ入力装置に接続され、前記コンピュータ・システムの動作中にプログラムを実行し、かつデータを処理する、前記格納装置内に装着されたシステム・プロセッサと、

前記システム・プロセッサに接続され、前記コンピュータ・システムの動作のためのプログラムを記憶する、前記格納装置内に装着された読取専用記憶素子（ＲＯＭ）と、

前記システム・プロセッサに接続され、プログラム及びデータを記憶し検索するためのシステム区画を有し、ユーザが除去する上でアクセスすることができない、前記格納装置内に装着された大容量記憶装置とを具備し、

前記コンピュータ・システムのユーザによる命令の入力に応答して、前記システム・プロセッサの解釈及び動作を可能にするインタープリタ・プログラムを前記ＲＯＭ素子内に記憶し、

複数のソース中の選択された１つからオペレーティング・システムを初期ロードし、該複数のソース中のどのオペレーティング・システムへもアクセスできない場合には、最後の選択デフォールトとして前記インタープリタ・プログラムを指定する、優先初期ローディング・プログラムを、前記ＲＯＭと前記大容量記憶装置のシステム区画のいずれかに記憶し、

前記複数のソースのグループから前記インタープリタ・プログラムを削除することによって、システム・オーナーと特権ユーザのいずれかが選択的に前記優先初期ローディング・プログラムを変更することを可能にする、セキュリティ・ユーティリティ・プログラムを、前記ＲＯＭと前記大容量記憶装置の前記システム区画のいずれかに記憶する、

コンピュータ・システム。

【請求項２】前記セキュリティ・ユーティリティ・プログラムが、

前記複数のソースのグループの番号と優先順序を指定することによって、システム・オーナーと特権ユーザのいずれかが、選択的に前記優先初期ローディング・プログラムを変更することを可能にする、

請求項１に記載のコンピュータ・システム。

【請求項３】前記セキュリティ・ユーティリティ・プログラムが、

コンピュータ・システムの一般ユーザ及び無許可ユーザのどちらによってもアクセス不能である、

請求項１または２に記載のコンピュータ・システム。

【請求項４】前記システム・プロセッサにより処理されるデータを暗号化する場合及び非暗号化する場合に使用されるマスター暗号鍵データを、前記コンピュータ・システム内に記憶し、

システム・オーナー及び特権ユーザのいずれかが該マスター暗号鍵データを変更することを可能にする第２のセキュリティ・ユーティリティ・プログラムを、前記大容量記憶装置の前記システム区画内に記憶する、

請求項１、２、または３に記載のコンピュータ・システム。

【請求項５】ユーザ入力のための入力装置と、

通常は閉じられている格納装置と、

前記入力装置に接続され、コンピュータ・システムの動作中にプログラムを実行し、かつデータを処理する、前記格納装置内に装着されたシステム・プロセッサと、

前記システム・プロセッサに接続され、前記コンピュータ・システムの動作のためのプログラムを記憶する、前記格納装置内に装着された読取専用記憶素子（ＲＯＭ）と、

前記システム・プロセッサに接続され、プログラム及びデータを記憶し検索するためのシステム区画を有し、ユーザが除去する上でアクセスすることができない、前記格納装置内に装着された大容量記憶装置とを具備し、

前記コンピュータ・システムのユーザによる命令の入力に応答して、前記システム・プロセッサの解釈及び動作を可能にするインタープリタ・プログラムを前記ＲＯＭ素子内に記憶し、

複数のソース中の選択された１つからオペレーティング・システムを初期ロードし、該複数のソース中のどのオペレーティング・システムへもアクセスできない場合には、最後の選択デフォールトとして前記インタープリタ・プログラムを指定する、優先初期ローディング・プログラムを、前記ＲＯＭと前記大容量記憶装置のシステム区画のいずれかに記憶し、

前記システム・プロセッサにより処理されるデータを暗号化する場合及び非暗号化する場合に使用されるマスター暗号鍵データを、前記コンピュータ・システム内に記憶する、コンピュータ・システムにおいて、

システム・オーナーと特権ユーザのいずれかが、

（ａ）前記複数のソースのグループの番号及び優先順序を指定することによって、前記優先初期ローディング・プログラムを選択的に変更し、

（ｂ）前記複数のソースのグループから前記インタープリタ・プログラムを削除することによって、前記優先初期ローディング・プログラムを選択的に変更することを可能にする、一般ユーザと無許可ユーザのいずれによってもアクセス不能の、前記大容量記憶装置の前記システム区画に記憶された第１のセキュリティ・ユーティリティ・プログラムを使用する段階と、

システム・オーナーと特権ユーザのいずれかが、前記マスター暗号鍵データを変更することを可能にする、前記

大容量記憶装置の前記システム区画内に記憶された第２のセキュリティ・ユーティリティ・プログラムを使用する段階とを有する、
コンピュータ・システムのセキュリティ機構の管理方法。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、パーソナル・コンピュータ・システムに関し、特にそのシステム内に保存されているデータへのアクセスにおける制御を可能にするセキュリティ機構を有するパーソナル・コンピュータ・システムに関するものである。

【０００２】

【従来の技術】一般的なパーソナル・コンピュータ・システム、特に×××のパーソナル・コンピュータが、現代社会における多くの分野においてその機能を発揮して広く利用されてきている。パーソナル・コンピュータ・システムは、通常、デスク・トップ型、床置き型、あるいは携帯用マイクロコンピュータとして定義することができ、一つのシステム・プロセッサと関連する揮発性及び不揮発性の記憶素子、表示モニタ、鍵盤装置、一つ以上のディスク駆動機構、固定ディスク記憶装置、及び選択的な印刷装置から成るシステム・ユニットから構成される。これらのシステムの顕著な特徴の一つは、これらの構成部品を互いに電気的に結合するためのマザーボード（ここでいうのは、システム・ボード、システム・プレーナ、あるいは、プレーナとして知られているもの）の使用である。これらのシステムは、基本的には、ひとりのユーザに独立した計算能力を提供し、個人及び小企業においても安価に購入できる価格に設計されている。そのようなパーソナル・コンピュータ・システムの例として、×××のパーソナル・コンピュータＡＴおよびパーソナル・システム／２（ＰＳ／２）モデル２５、３０、３５、４０、Ｌ４０ＳＸ，５０、５５、５６、５７、６５、７０、８０、９０、９５がある。

【０００３】これらのシステムは、一般に二つの群に分類される。一つは、ファミリＩ型と通常言われており、×××のパーソナル・コンピュータＡＴ及び他の”ＩＢＭ互換”機に代表されるバス・アーキテクチャを使用している。もう一つは、ファミリＩＩ型といわれており、×××社のパーソナル・システム／２モデル５０～９５に代表されるマイクロ・チャネル・バス・アーキテクチャを使用している。初期のファミリＩ型は、通常、一般的な×××××の８０８８か８０８６をシステム・プロセッサのマイクロプロセッサとして使用していた。後のファミリＩおよびファミリＩＩ型のあるものは、高速の×××××の８０２８６、８０３８６、８０４８６のマイクロプロセッサが通常使用され、それによって、実モードにおいては低速の×××××８０８６マイクロプロセッサをエミュレートし、あるいは保護モードにおいては、アドレス範囲を１ＭＢから４ＧＢに拡張する操作が、いくつかの型について可能である。つまり、８０２８６、８０３８６、８０４８６マイクロプロセッサの実モードの機能は、８０８６及び８０８８用に書かれたソフトウェアについて、ハードウェアの互換性を提供することである。

【０００４】近年世界的にパーソナル・コンピュータが発展し、利用されてくるとともに、膨大なデータや情報が収集されて、そのようなシステム内に保有されまた記憶されてきている。このデータの多くは、性質として機密を要するものである。取り扱いを誤ると、データが個人にとって困惑するものになったり、企業が競争力を失ったり、あるいは、個人に対する肉体的暴力を引き起こしたりする。ユーザがデータの機密性及びその価値をさらに認識するようになるにつれ、そのような誤った使用に対する保護が一層要求されてくる。記憶されたデータ及びそれに関連する人間を保護するために、ユーザは、自分の購入するパーソナル・コンピュータの中に、セキュリティ機構と保全性機構を組み込むことを要求している。

【０００５】収集され、記憶されるデータの機密性を重要視するのは、ユーザのみではない。政府もまた、機密データの保護を強化する法律を施行しつつある。それは合衆国政府だけではない。その現状の重要性が認識されそれに対応するようになった。合衆国連邦政府は、セキュリティ・レベルとこれらのレベルに適応させるための関連する必須要件を定め、パーソナル・コンピュータ製品を製造する業者に対して、その製品が、その業者の申請したセキュリティ・レベルに合っているかどうかを検査するための認可機関を設立している。Ｆｅｄｅｒａｌ Ｒｅｑｕｉｒｅｍｅｎｔｓの基本は、国防省の、トラステッド・コンピュータ・システム評価基準（Ｔｒｕｓｔｅｄ Ｃｏｍｐｕｔｅｒ Ｓｙｓｔｅｍ Ｅｖａｌｕａｔｉｏｎ Ｃｒｉｔｅｒｉａ）、ＤＯＤ ５２００．２８ ＳＴＤ１２／８５であり、一般にオレンジブックといわれているものである。政府は、１９９２年１月１日より、政府に関するすべてのデータは、パーソナル・コンピュータにおいてはセキュリティレベルＣ－２以上でのみ処理され、記憶されなければならないという法律を制定した。コンピュータシステムのハードウェアにおいては、この必須要件は、本質的に保証セクション内に含まれる。必須要件６には、”信頼できる機構は、不正及びまたは不当な変更に対して、絶え間なく保護されなければならない。・・・”とある。

【０００６】最も初期の、×××パーソナル・コンピュータでいえばファミリＩ型のパーソナル・コンピュータ・システムについてみると、ソフトウェアの互換性が最も重要であると考えられていた。この目的を達成するため、”ファームウェア”とも言われている絶縁層のシステム常駐コードが、ハードウェアとソフトウェアの間に

確立されている。このファームウェアは、ユーザのアプリケーション・プログラムやオペレーション・システムと入出力装置の間の操作インターフェースを提供し、ユーザが、ハードウェア装置の特性について意識しなくてもよいようにしている。最終的にこのコードは、システムに新しい入出力装置を追加できるようにする一方、アプリケーション・プログラムをハードウェアの特異性から絶縁する、基本入出力システム（ＢＩＯＳ）内として開発されることとなった。ＢＩＯＳの重要性は、即座に明らかになった。なぜなら、それによって、入出力装置駆動機構が、特定の入出力装置のハードウェアに依存しなくても良く、また入出力装置駆動機構に入出力装置との中間的なインターフェースを付けなくても良いからである。ＢＩＯＳはシステムに統合された一部であり、システム・プロセッサのデータの入出力の移動を制御されるので、システム・プレーナ上に設置され、読取専用記憶素子（ＲＯＭ）としてユーザに出荷される。例えば、原型のＸＸＸパーソナル・コンピュータ内のＢＩＯＳは、プレーナ・ボード上に設置されたＲＯＭの８Ｋバイトを占めていた。

【０００７】パーソナル・コンピュータ・ファミリの新機種が登場すると、ＢＩＯＳは、新しいハードウェア及び入出力装置を搭載するために改良され、拡張されなければならなかった。予測されたとおり、ＢＩＯＳは、記憶素子の量を増加し始めた。例えば、ＸＸＸのパーソナル・コンピュータＡＴの導入によって、ＢＩＯＳはＲＯＭの３２Ｋバイトを必要とするようになった。

【０００８】今日、新技術の開発により、ファミリＩＩ型パーソナル・コンピュータ・システムは非常に精巧になって進歩し、消費者にも入手しやすくなっている。技術が急速に変わり、新しい入出力装置がパーソナル・コンピュータ・システムに加わっているため、ＢＩＯＳの変更が、パーソナル・コンピュータ・システムの開発サイクルの中で重要な問題になってきた。

【０００９】例えば、マイクロ・チャネル・アーキテクチャを持つＩＢＭのパーソナル・システム／２においては、拡張ＢＩＯＳあるいはＡＢＩＯＳとして知られる非常に新しいＢＩＯＳが開発された。しかしながら、ソフトウェアの互換性を維持するために、ファミリＩ型からのＢＩＯＳを、ファミリＩＩ型にも組み込む必要があった。ファミリＩ型のＢＩＯＳは、互換ＢＩＯＳ、あるいはＣＢＩＯＳとして知られている。しかし、先に述べたように、ＸＸＸのパーソナル・コンピュータＡＴは、３２ＫバイトのＲＯＭしか、プレーナ・ボード上に設置されていない。幸いに、このシステムはＲＯＭを９６Ｋバイトまで拡張できるが、不運な点は、システムの制限のため、この９６Ｋバイトが、ＢＩＯＳに与えることのできる最大の容量であることがわかったことである。運良く、ＡＢＩＯＳ及びＣＢＩＯＳは、まだ９６ＫバイトのＲＯＭの中に押し込むことができた。しかしながら、９６ＫバイトのＲＯＭ領域のうちわずかな部分しか拡張のために残らなかった。将来的な入出力装置の追加については、最終的にＣＢＩＯＳおよびＡＢＩＯＳが、ＲＯＭ空間からあふれてしまうと確信されている。このように、新しい入出力技術は、容易にはＣＢＩＯＳ及びＡＢＩＯＳ内に統合することができないであろう。

【００１０】これらの問題、及び開発サイクル内でできるだけ最新のファミリＩＩ型ＢＩＯＳにおいて変更を行いたいという要望のために、ＲＯＭからＢＩＯＳ部をオフロードすることが必要になった。このことは、ＢＩＯＳ部を固定ディスクのような大容量記憶装置上に、好ましくはシステム区画として知られるそのようなディスクの定義された部分に記憶することで達成された。このシステム区画はまた、システム参照ディスケットのイメージも記憶しており、それは、システム構成などを確立する際に用いられるある種のユーティリティ・プログラムを含んでいる。ディスクは読取りと同様に書込みも可能なので、ディスク上の実際のＢＩＯＳコードを変更することは実現可能になった。ディスクは、高速で効率の良い方法でＢＩＯＳコードを記憶できるが、それにもかかわらず、ＢＩＯＳコードが不良になる可能性が非常に大きくなった。ＢＩＯＳは、オペレーティング・システムに統合された一部であるため、ＢＩＯＳの不良によって、破壊的な結果を生じ、多くの場合システムが完全に故障及び操作不能になる。このように、固定ディスク上のＢＩＯＳコードの不当な変更を防ぐための手段が、切実に望まれていることが、明らかとなった。これは、８９年８月２５日出願の米国出願３９８，８２０号で１９９１年６月４日に特許された米国特許５，０２２，０７７号の解決しようとする課題である。この特許を参照すれば、本発明を理解するのに役立つ付加的情報が得られる。またこの特許の開示内容は、ここに開示された本発明の完全な理解のためこの明細書中に必要な部分を参照することとする。

【００１１】ＸＸＸのＰＳ／２の導入によって、マイクロ・チャネル・システムは、入出力カード及びプレーナからスイッチとジャンパを取り除いた。マイクロ・チャネル・アーキテクチャは、それらに替わってプログラム可能なレジスタを提供する。このため、これらのプログラム可能なレジスタあるいはプログラマブル・オプション・セレクト（ＰＯＳ）レジスタを構成するためのユーティリティが、必要となった。これらのユーティリティ、及び他のユーティリティは、システムの診断に従って、システムの使用性を向上させるためのものであり、それぞれのシステムにおいて、システム参照ディスケットの上に搭載される。

【００１２】最初の使用に先立って、それぞれのマイクロ・チャネル・システムは、そのＰＯＳレジスタを初期化する必要がある。例えば、システムに新しい入出力カードを立ち上げた場合、あるいは入出力カード用のスロ

ットを変えた場合、構成エラーが発生し、そのシステム立ち上げ手続きが停止する。ユーザは、それからシステム参照ディスケットをロードし、Ｆ１キーを押すように指示される。そうすると、”構成設定ユーティリティ”をシステム参照ディスケットから立ち上げることができ、システムを構成する。構成設定ユーティリティは、ユーザに対し必要な操作を指示する。もし適当な入出力カードの記述ファイルが、システム参照ディスケット上にロードされれば、構成設定ユーティリティは、正しいＰＯＳあるいは不揮発性記憶素子内の構成データを作成する。記述ファイルは、そのカードのシステムへのインターフェースのための構成情報を含んでいる。

【００１３】

【発明が解決しようとする課題】本発明の目的は、パーソナル・コンピュータ・システム内に保存されているデータへのアクセスを制御することのできるセキュリティ機構を提供することにある。特に、本発明は、知識のあるユーザが本来なら安全保護されるパーソナル・コンピュータ・システムに入り込むことを可能にする命令を直接入力できるインタープリタ・プログラムを、利用不能にすることを目的とする。同様に、本発明は、パーソナル・コンピュータ・システムの記憶素子内に保存されているマスター暗号鍵を保護することを目的とする。

【００１４】

【課題を解決するための手段】本発明は、システム・オーナーや特権ユーザに対し、パーソナル・コンピュータ・システムが、従来のそのパーソナル・コンピュータ・システムの特性に関する知識を持った攻撃者（侵害者）によるアクセスに対しても適切に安全保護される一方、知識のあるユーザに知られている特性についてはシステムが安全保護されないことを保証するための管理手段を提供する。

【００１５】特定のユーザが、（ａ）複数のソースの番号と優先順序を特定することによって、初期ローディング・プログラムを選択的に変更できるための、及び

（ｂ）複数のソースからインタープリタ・プログラムを削除することによって、初期ローディング・プログラムを選択的に変更できるための、セキュリティ・ユーティリティ・プログラムと、システムＣＰＵによって処理されるデータを暗号化する場合及び非暗号化する場合に使用するためのマスター暗号鍵と、特定のユーザがマスター暗号鍵を変更できるための、第２のセキュリティ・ユーティリティ・プログラムを有するパーソナル・コンピュータ・システムである。

【００１６】

【実施例】以下に本発明を、好ましい実施例を示した図を参照してより詳細に記述するが、説明を始めるにあたって、適切な当業者であれば本発明の有用な効果を得ようとしてここに記述された発明を修正することもあると考えられる。したがって、以下の記述は、一般的な技術者に指示するための大まかな、説明のための開示であって、本発明を限定するものではない。

【００１７】以下の、いくつかの定義された用語がここで使用される。

【００１８】トラステッド・コンピューティング・ベース（ＴＣＢ）：　コンピュータ・システム内の保護機構全体であり、ハードウェア、ファームウェア、ソフトウェアを含む。それらの組合せが、セキュリティ方策（security policy）の強制に対して責任を追う。ＴＣＢは一つ以上の構成部分からなり、それらがまとまって製品あるいはシステム全体の統合されたセキュリティ方策を強制する。セキュリティ方策を正確に強制するためのＴＣＢの能力は、ＴＣＢ内の機構とシステム管理人によるセキュリティ方策に関するパラメータ（例えばユーザの取り扱い許可）のみに依存する。

【００１９】トラステッド・ソフトウェア：　トラステッド・コンピューティング・ベース（ＴＣＢ）のソフトウェア部分。

【００２０】トラステッド・プログラム：　トラステッド・ソフトウェアに含まれるプログラム。

【００２１】オープン・プログラム：　トラステッド・コンピューティング・ベース（ＴＣＢ）上で操作できるプログラムで、トラステッド・プログラム以外のもの。

【００２２】参照モニタ・コンセプト：　サブジェクトによるオブジェクトへのすべてのアクセスを調停する抽象マシンを参照するアクセス制御構想。

【００２３】セキュリティ・カーネル：　参照モニタ・コンセプトを実行するトラステッド・コンピューティング・ベースのハードウェア、ファームウェア、ソフトウェアの要素である。これは、すべてのアクセスを調停し、変更から保護され、かつ、正確なものと確証可能でなければならない。

【００２４】トラステッド・コンピュータ・システム：　機密性のある、あるいは分類された情報の領域を同時に処理するために使用できる、十分なハードウェアとソフトウェアの保全手段を備えたシステム。

【００２５】システム・オーナー：　システム・オーナーは、最初に、安全保護モードにシステムを構成し設置する責任のあるユーザである。システム・オーナーは、初期設定時及び必要なときはいつでも構成を制御する。システム・オーナーは、特権アクセス・パスワードを制御しまたその保全性を維持する責任がある。システムオーナーはまた、不正検知カバー錠機構の鍵の物理的セキュリティを図る責任を負う。システム・オーナーは、すべてのシステム上の経過記録のセキュリティにも責任がある。システム・オーナーは、一つ以上のシステムを所有することがある。システム・オーナーは、特権ユーザと考えられ、かつ一般ユーザであっても良い。

【００２６】安全保護モード：　セキュリティ要素及び保全性要素によって提供されるセキュリティ保護を呼込

むために、システム・オーナーが、パーソナル・コンピュータ上に、首尾よく特権アクセス・パスワードを導入したときのモード。

【００２７】特権ユーザ：　特権アクセス・パスワードの使用を許可されたすべてのユーザ。特権ユーザは、システム・オーナーであってもなくても良い。特権ユーザは、特定のあるいは一組のシステムの鍵を所有しても良い。セキュリティの漏洩からシステムを回復する際に、特権ユーザが関係する場合は、そのことをシステム・オーナーに報告する責任がある。特権ユーザは、一般ユーザであっても良い。

【００２８】一般ユーザ：　システム機能を使用することを許可されたすべてのユーザ。システム構成を変更するため、あるいは問題を特定するために、一般ユーザは、システム・オーナーあるいは特権ユーザに援助を求める。一般ユーザは、特権ユーザかシステム・オーナーを兼ねていないかぎり、特権アクセス・パスワードあるいは不正検知カバー錠機構の鍵（tamper evident cover keylock key）を所有していない。

【００２９】無許可ユーザ：　システム・オーナー、特権ユーザ、一般ユーザ以外のすべての者。安全保護されたパーソナル・コンピュータ・システムにおける無許可ユーザによるどのような使用も、電源が起動しなかった場合を除いて、セキュリティの漏洩とみなされる。そのような漏洩を明らかにするために追跡監査が行われなければならない。

【００３０】ＥＥＰＲＯＭ：　電気的に書換え可能な読取専用記憶素子。この記憶素子技術によって、データの不揮発性記憶が、ハードウェア論理の制御の下で変更可能になる。記憶素子の内容は、電源を切っても失われない。その内容は、モジュールへの適切な制御信号が、あらかじめ決められた手順で与えられたときのみ、書換えられる。

【００３１】パスワード記述：　システムは、二つのパスワードによって保護される機能を有している。即ち、一つは、特権アクセス・パスワード（ＰＡＰ）、もう一つはは、電源起動パスワード（ＰＯＰ）である。これらのパスワードは、互いに独立に使用されるようになっている。ＰＡＰは、初期プログラムロード（ＩＰＬ）装置立上げリスト、パスワード・ユーティリティへのアクセス、及びシステム参照ディスケットあるいはシステム区画へのアクセスを保護することによって、システムオーナーを保護できるように設計されている。システム区画は、ＰＡＰが導入されていないかあるいは電源起動手順の間にＰＡＰが初期入力された場合に、ＰＯＳＴエラーに応答して（あるいはウォーム立上げの際）のみ立ち上げられる。ディスケットからの初期ＢＩＯＳロード（ＩＢＬ）は、システム参照ディスケットを立ち上げるのと同じ方法で安全保護を図られる。ＰＡＰの存在は、ＰＯＰを使用する一般ユーザには意識されない。ＰＡＰは、システム参照ディスケットあるいはシステム区画内のユーティリティによって導入、変更、あるいは削除される。ＰＡＰが正しくセットされて入力されたとき、ＰＯＰに優先して、オーナーは、システム全体にアクセスできる。ＰＯＰは、現在のすべてのＰＳ／２システム上で有効であり、ＤＡＳＤ上のオペレーティング・システムあるいはシステム機能への無許可のアクセスを防ぐために使用される。

【００３２】添付の図面を参照すると、本発明を実施したマイクロコンピュータが、図１の１０で示されている。上記したように、コンピュータ１０は、関連するモニタ１１、鍵盤装置１２、及び印刷装置又はプロッタ１４を備えている。図２に示すように、コンピュータ１０は、シャーシ１９と組み合わされたカバー１５を有し、デジタル・データを処理及び記憶するための電気的に稼働するデータの処理及び記憶部品を収納する、外装されシールドされた本体を形成する。。図２に示された形態では、コンピュータ１０はまた、随意の入出力ケーブル接続のカバー１６を有し、コンピュータシステムの入出力ケーブルの接続部を覆い、保護している。少なくともある種のシステム部品は、多層プレーナ２０（ここでは、マザーボードあるいはシステム・ボードともいう）上に装着されている。多層プレーナは、シャーシ１９に取り付けられ、先に明示したもの及びフロッピ・ディスク装置、種々の形の直接アクセス記憶装置、アクセサリー・カードあるいはボード等の関連素子を含むコンピュータ１０の構成部品を電気的に内部接続するための手段となっている。

【００３３】シャーシ１９は、底面及び背面パネル（図２のように、ケーブル接続カバー１６で外部を覆われる場合もある。）を有し、磁気あるいは光学ディスク、テープ・バックアップ装置などのためのディスク装置のようなデータ記憶装置を収納するために、少なくとも一つの空いた部分を設定している。図示された形態では、上部の空間２２は、ある大きさの周辺機器駆動機構（３．５インチ駆動機構として知られている様なもの）を受容するのに適合している。フロッピー・ディスク装置は、この上部空間２２に備え付けても良い。それは、一般に知られているように取り外しできる媒体の直接アクセス記憶装置で、その中にディスケットを挿入することができ、またデータを受信し、記憶し、送り出すためにディスケットを使用することができる。

【００３４】上記の構造を本発明と関連付ける前に、パーソナル・コンピュータ・システム１０の一般的な操作の概要を、説明する。図３は、本発明に沿ったシステム１０のようなコンピュータ・システムの種々の構成部分を図示したパーソナル・コンピュータ・システムのブロック図である。その中には、プレーナ２０に装着された構成部分、プレーナの入出力スロットへの接続部、及び他のパーソナル・コンピュータ・システムのハードウェ

アが含まれる。プレーナに接続されているのは、システム・プロセッサ３２である。ＣＰＵ３２としては、適当なマイクロプロセッサを用いることができる。適当なマイクロプロセッサの一つは、×××××社の８０３８６である。ＣＰＵ３２は、高速ＣＰＵローカル・バス３４によって、バス・インターフェース制御ユニット３５、ここではシングル・インライン記憶素子モジュール（ＳＩＭＭ）として示されている揮発性ランダム・アクセス記憶素子（ＲＡＭ）３６、及びＣＰＵ３２への基本入出力操作のための命令を記憶したＢＩＯＳ　ＲＯＭ３８に接続される。ＢＩＯＳ　ＲＯＭ３８は、入出力装置とのインターフェースに使用されるＢＩＯＳとマイクロプロセッサ３２のオペレーティング・システムを含む。ＲＯＭ３８はまた、パーソナル・コンピュータ・システムのユーザが直接的に入力した指令に応答して、ＣＰＵ３２が解釈及び操作を実行できるようにその中にインタープリタ・プログラムを記憶している。従来は、インタープリタ・プログラムは通常、鍵盤装置の文字入力を受取り、初心者用で用途の広い記号による命令コード（ＢＡＳＩＣ）を解釈することができた。しかしながらこのプログラムは、他の形式の命令入力そしておそらくは他のコードが使用されることを想定したものである。例えば、命令入力は、音声認識による音響入力システムか、あるいは手書きによるペンまたはポイントへのタッチで入力するシステムによるものでもよい。本明細書においては、全てのそのような入力装置を「ユーザ入力装置」として参照し、そしてコンピュータが認識できる入力は「命令」として参照する。ＢＩＯＳ　ＲＯＭ３８に記憶された命令は、ＢＩＯＳの実行時間を短縮するためにＲＡＭ３６内に複写することができる。またシステムは、汎用性を持たせるためバッテリー付きの不揮発性記憶素子（普通は、ＣＭＯＳ　ＲＡＭ）を備えた回路部品を有しており、それによって、システム構成と実時間クロック（ＲＴＣ）６８（図３及び図４）に関するデータを受信したり保存したりする。

【００３５】本発明を、特に図３のシステムブロック図を参照して説明する。以下に続く説明によって、本発明による装置及び方法が、プレーナ・ボードの他のハードウェア構成にも使用できることが理解される。例えば、システム・プロセッサは、×××××の８０２８６あるいは８０４８６マイクロプロセッサでも良い。

【００３６】図３に戻って、ＣＰＵローカルバス３４（データ、アドレス、制御部分から成る）によって、マイクロプロセッサ３２を、数値演算コプロセッサ３９及び小型コンピュータ・システム・インターフェース（ＳＣＳＩ）制御装置４０とも接続できる。ＳＣＳＩ制御装置４０は、コンピュータ設計及び操作技術者には知られているが、ＲＯＭ４１、ＲＡＭ４２、及び図３右側に示された入出力接続部によって種々の型式の適当な内部あるいは外部装置へ容易に接続され、また接続可能である。ＳＣＳＩ制御装置４０は、固定及び着脱可能な媒体の電気磁気的記憶装置（ハード及びフロッピーディスク駆動機構としても知られる）、電気光学的、テープ及び他の記憶装置等の記憶装置を制御する場合の、記憶装置制御装置として機能する。本発明においては、そのような記憶装置の中の少なくとも１つは、システム格納装置内に装着された大容量記憶装置であり、ユーザはこれを除去するためのアクセスをすることができない。この特別に識別された大容量記憶装置は、システム区画を有しており、操作によってＣＰＵ３２と接続されて、プログラムやデータをその中に記憶しまたその中からプログラムやデータを検索する。システム区画を有する装置の重要性は、以上に簡単に述べたとおりである。この装置へユーザがアクセスすることができないことの重要性は、即ち、システム・セキュリティ機構によってこの装置が不正あるいは除去及び交換のための物理的アクセスから保護されていることである。

【００３７】本発明の出願人による前述の出願に記載されているように、パーソナル・コンピュータを動作状態にするプロセスは、当業者には一般的に理解されている特有の専門用語によって明確にされている一連の段階を経て進行する。従って、当業者であれば、ＰＯＳＴ（パワーオン自己検査）、ＩＭＬ（初期マシン・ロード）、ＩＰＬ（初期プログラム・ロード）は理解できるはずである。ＰＯＳＴはＩＭＬを呼出し、ＩＭＬはＩＰＬを呼出し、そしてＩＰＬはオペレーティング・システムをロードし、パーソナル・コンピュータを動作状態にする。ＰＯＳＴ、ＩＭＬ、ＩＰＬの各部は、前記のＲＯＭ３８とシステム区画に配分してもよい。ＩＭＬは、ＲＡＭ（ここでは、ＳＩＭＭ３６）の指定領域へ、実行時ＢＩＯＳのイメージ、上記のインタープリタ・プログラム、及びＰＯＳＴの一部をロードする。ＩＰＬは、システム・オーナによって与えられた優先リスト上で識別されたソースから指定されたオペレーティング・システムをロードする。この識別機能は、ここでは「優先初期ローディング・プログラム」として参照される。

【００３８】通常は、初期ローディング・プログラムは、大容量記憶装置のシステム区画内に記憶されており、システム１０の（例えば）立ち上げ可能な大容量記憶装置もしくはフロッピー・ディスク駆動装置に装着されたディスケット、大容量記憶装置のシステム区画、及びフロッピー・ディスク駆動装置の適当な場所に装着された参照ディスケットを含む複数のソースの内の選択された１つから、オペレーティング・システムを初期ロードすることができる。優先初期ローディング・プログラムは、通常、このような複数のソースのどのオペレーティング・システムへもアクセスできない場合に、最後の選択として、ＲＯＭ３８に記憶されているかあるいはＲＡＭ内にロードされている例えばＢＡＳＩＣのインタープリタ・プログラムを指定する。

【００３９】バス・インターフェース制御装置（ＢＩＣ）３５は、ＣＰＵローカルバス３４と入出力バス４４を結合する。バス４４によって、ＢＩＣ３５は、マイクロ・チャネル・バスのような選択機構バスと結合される。マイクロ・チャネル・バスは、マイクロ・チャネル・アダプタ・カード４５を収納するための複数の入出力スロットを有し、マイクロ・チャネル・アダプタ・カード４５はさらに、入出力装置あるいは記憶装置（図示せず）に接続されることもある。入出力バス４４は、アドレス、データ、及び制御要素を含む。

【００４０】入出力バス４４に沿って結合されているものは、画像信号処理装置（ＶＳＰ）４６のような種々の入出力部品である。画像信号処理装置４６は、グラフィック情報を記憶し（４８で示す）またイメージ情報を記憶する（４９で示す）ビデオＲＡＭ（ＶＲＡＭ）に関係する。処理装置４６によって交換された画像信号は、ディジタル・アナログ変換器（ＤＡＣ）５０を通してモニタまたは他の表示装置へ送られる。ＶＳＰ４６を、カメラなどの画像記録再生装置の形態を取る、いわゆる自然な入出力と直接に接続することも可能である。入出力バス４４はまた、ソフトウェア命令を記憶できる命令ＲＡＭ５２とデータＲＡＭ５４に関連するディジタル信号処理装置（ＤＳＰ）と結合されている。ソフトウェア命令は、ＤＳＰ５１による信号処理とその処理に含まれるデータ処理のために使用される。ＤＳＰ５１によって、音声制御装置５５の設置による音声入力及び出力の処理ができる。また、アナログ・インターフェース制御装置５６に設置による他の信号も扱える。最後に、入出力バス４４は、入出力制御装置５８に結合される。入出力制御装置５８は、関連する電気的に書換え可能な読取専用記憶素子（ＥＥＰＲＯＭ）５９を持ち、それによって入力及び出力を、汎用的な周辺機器と交換する。周辺機器には、フロッピー・ディスク駆動装置、印刷装置あるいはプロッタ１４、鍵盤装置１２、マウスあるいはポインティング（図示せず）が含まれ、シリアル・ポートによって行う。ＥＥＰＲＯＭは、後述するセキュリティ機構の中で機能し、それによって入力及び出力を、通常の周辺機器と交換する。周辺機器には、フロッピー・ディスク駆動装置、印刷装置あるいはプロッタ１４、鍵盤装置１２、マウスあるいはポインティング（図示せず）、他のマルチメディア入力装置（図示せず）が含まれ、シリアル・ポートによって行う。ＥＥＰＲＯＭは、米国特許出願第８４０、９６５号（１９９２年２月２６日出願）に基づく特願平４－３４１８０５号に記載されるようなセキュリティ機構の中で機能する。いずれにしても、多層化されたパスワード保護に関するより詳細な議論はこの出願を参照されたい。

【００４１】以後、さらに詳細に述べられる本発明の目的の達成において、パーソナル・コンピュータ・システム１０は、システム格納装置内に装着された書換え可能な記憶素子を有する。この記憶素子は、活動状態と非活動状態を選択的に操作し、活動状態にあるときに、特権アクセス・パスワード（後により厳密に説明する）を受信し記憶するためのものである。書換え可能な記憶素子は、好ましくは、上記の電気的に書換え可能な読取専用記憶素子あるいはＥＥＰＲＯＭ５９（図３）である。システムはまた、格納装置内に装着された選択スイッチあるいはセキュリティ・スイッチを有している。当該スイッチは操作により（operatively）、書換え可能な記憶素子５９と接続され、記憶素子を活動状態及び非活動状態にセットする。選択スイッチ（本明細書の中ではセキュリティ・スイッチともいう）は、例えば、システム・プレーナ２０上に装着されたジャンパであって、プレーナにアクセスする人間の手動によって二つの状態にセットできるものがある。一つの状態（書込み可能状態ともいわれる）において、ＥＥＰＲＯＭ５９は活動状態にセットされ、ここで記述したＰＡＰを記憶する。書込み可能状態では、ＰＡＰをＥＥＰＲＯＭに書込み、変更、あるいは削除することができる。他の状態または非活動状態では、ＥＥＰＲＯＭのＰＡＰ記憶能力は、非活動状態にセットされる。

【００４２】上記したように、システム１０はまた、書換え可能な記憶能力を有する第２の構成要素を備えている。いわゆるバッテリ付きの不揮発性ＣＭＯＳ　ＲＡＭ及び関連する実時間クロック（ＲＴＣ）であり、図４中に６８で示されている。ＣＭＯＳ　ＲＡＭは、システム構成を表すデータを記憶する。本発明においては、それは、システム１０の電源起動時に、正しくＰＡＰを入力することに関するデータを含む。少なくとも一つの不正検知スイッチ（図４、５、６）が格納装置内に装着されて提供されており、操作によりＣＭＯＳ　ＲＡＭと接続されて、格納装置が開けられたことを検知する。また不正検知スイッチが入ることに応答してその記憶素子内に記憶された特定のデータをクリアする。

【００４３】上記の、及び後述する新しいセキュリティ機構及び保全機構は、先に提示されたパーソナル・コンピュータのセキュリティ機構である、電源起動パスワード（ＰＯＰ）とは独立に働く。これらの付加的なセキュリティ機構および保全機構は、オレンジ・ブック等で適用される規制の下でのオペレーティング・システム保証に対する、安全保護の土台となる。安全保護モードにシステムを設定するためには、さらにパスワードが必要である。新しいパスワードは、ここでは特権アクセス・パスワード（ＰＡＰ）といわれている。以前のパーソナル・コンピュータ・システムとの互換性を維持するために、ＰＯＰはなおサポートされる。本開示は、新しいセキュリティ機構及び保全機構について述べており、それは、ＥＥＰＲＯＭ、選択スイッチ、及び不正検知カバーを備えたパーソナル・コンピュータ・システム上で働くＰＯＳＴ及びパスワード・ユーティリティに関するもの

である。

【0044】パスワード・セキュリティはシステムのハードウェア機構によって実行される。即ち、EEPROM、セキュリティ・スイッチ、不正検知カバー・スイッチ、ファームウェア、POST、及びシステム・ソフトウェア・パスワード・ユーティリティである。PAPが、一旦導入されると、システムは安全保護モードになる。PAPはEEPROM内に保管される。PAPのバックアップ・コピーもまたEEPROM内に保持される。これは、PAPの導入、変更、あるいは削除の際に電源の故障が生じた場合、PAPが偶発的に失われるのを防ぐためである。POPと、PAP（導入された場合）の有効性を示す特定のビットは、CMOSRTCに記憶される。CMOS RTC内及びEEPROM内に保存されたデータの変更は、互いに独立している。

【0045】EEPROM中の二つのビットは、POSTに対して、現在の手順中に停電が生じたことを確実に知らせるための状態マシンとして用いられる。そして、可能であれば、システム・ボードの補助状態から復帰する。パスワード・ユーティリティは、PAPへのあらゆるアクセスの間に使用される二ビットの状態マシンである、更新標識フィールドを保持する。もし、パスワードの変更中に停電が生じたら、電源が回復したとき、POSTは状態マシンを検査する。（POSTは、実際には、電源起動時には常に検査を行う。）もしPAPが正しく更新された（'00'状態）なら、POSTは通常の方法で処理を続ける。もし、更新が停電の前に開始されていた（'01'状態）なら、POSTは有効なバックアップPAPの存在を検査する。もし有効であれば、POSTは、バックアップPAPを前のPAPについて記憶素子内に複写する。もし前のPAPが正しく更新された（'10'状態）なら、POSTは、当該前のPAP（新しいPAP）を用いて、システム参照ディスケットの使用やシステム区画の立上げを試みることを有効化する。POSTは、そのバックアップPAPは無効であるとみなす。POSTは、この場合、前のPAPをバックアップPAPに複写する。もし、選択スイッチあるいはセキュリティ・スイッチがロックされているか、書込み可能状態でなければ、エラーが表示される。システム・オーナーは、カバーの錠を外し、セキュリティ・スイッチの設定を変えることで対応しなければならない。

【0046】バックアップPAPが、正しく更新された（'11'の状態）ならば、前のPAP及びバックアップPAPは有効とみなされ、POSTは、ユーザによるPAP入力を確認する前に、前のPAPの有効性を照合する。

【0047】本開示において特に目的とするセキュリティ機構においては、セキュリティ・ユーティリティ・プログラムは、一般ユーザによっても無許可ユーザによってもアクセスすることのできない大容量記憶装置のシステム区画内に記憶されている。そして、システム・オーナーまたは特権ユーザが、下記のことを実行できる。

（a）複数の初期プログラム・ロード（IPL）のソース・グループの番号と優先順序を特定することによって、前記の優先初期ローディング・プログラムを選択的に変更すること。

（b）IPLのソース・グループからROM38内に記憶されたBASICのインタープリタ・プログラムを削除することによって、優先初期ローディング・プログラムを選択的に変更すること。

セキュリティ・コード化プログラムの制御下でCPU32によって処理されたデータを暗号化する場合及び非暗号化する場合に使用するために、パーソナル・コンピュータ・システム10の記憶場所に記憶されるデータの形式で、マスター暗号鍵が与えられている。このマスター暗号鍵は、特定のシステム10に固有のものである方が望ましいが、通常は、特権ユーザに割り当てられるかあるいは選択される一人一人の個人的な暗号鍵とともにアクセスされ、使用される。ここに開示されたように、多層化された暗号鍵の存在によって、トラステッド・コンピュータ・ベース上で保持されているコード化されたファイルへのアクセスにおける安全保護制御が保証される。

【0048】マスター暗号鍵が与えられている場合は、第2のセキュリティ・ユーティリティ・プログラムが大容量記憶装置のシステム区画内に記憶されており、システム・オーナーまたは特権ユーザがマスター暗号鍵のデータを変更することができる。

【0049】

【発明の効果】本発明によって、パーソナル・コンピュータ・システム内に保存されているデータへのアクセスを制御することのできるセキュリティ機構が提供される。

【図面の簡単な説明】

【図1】本発明の実施例であるパーソナル・コンピュータの透視図である。

【図2】シャーシ、カバー、及びプレーナ・ボードを含み、かつこれらの関係を示した図1のパーソナル・コンピュータの一部の展開透視図である。

【図3】図1及び図2のパーソナル・コンピュータの特定の部品の概略図である。

【図4】本発明のセキュリティ機構に関係する図1及び図2のパーソナル・コンピュータの特定の部品の概略表示である。

【図5】本発明のセキュリティ機構に関係する図1及び図2のパーソナル・コンピュータの特定の部品の概略表示である。

【符号の説明】

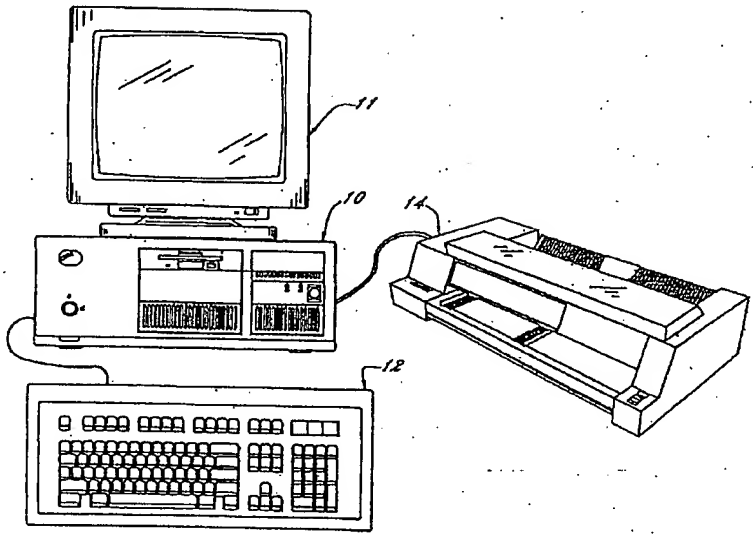
10　パーソナル・コンピュータ・システム

15　主カバー

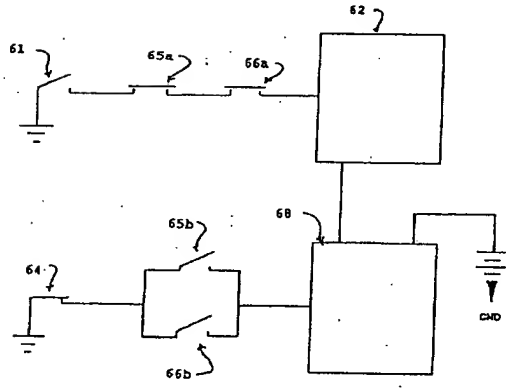
17　　18

１６　ケーブル接続カバー
１９　シャーシ
２０　多層プレーナ（マザー・ボード、またはシステム・ボード）
３８　ＢＩＯＳ　ＲＯＭ
５８　入出力制御装置
５９　ＥＥＰＲＯＭ
６１　システム電源のスイッチ
６２　システム電源
６４　錠スイッチ
６５　カバースイッチ
６６　選択的カバースイッチ
６８　ＣＭＯＳ　ＲＡＭおよび実時間クロック（ＲＴＣ）

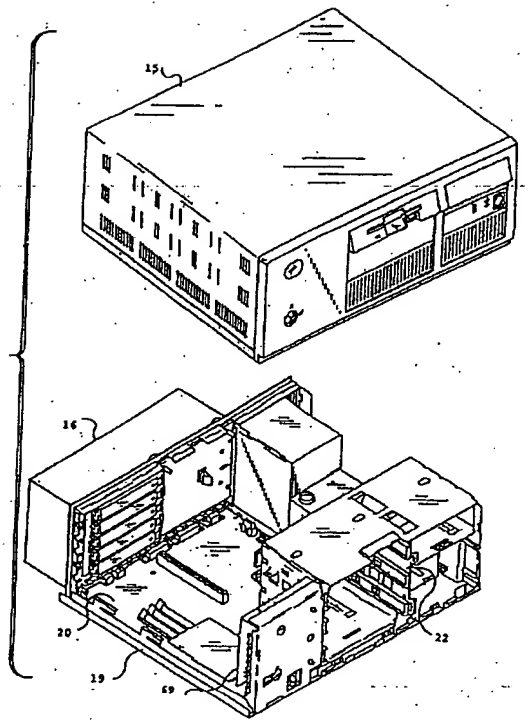
【図１】



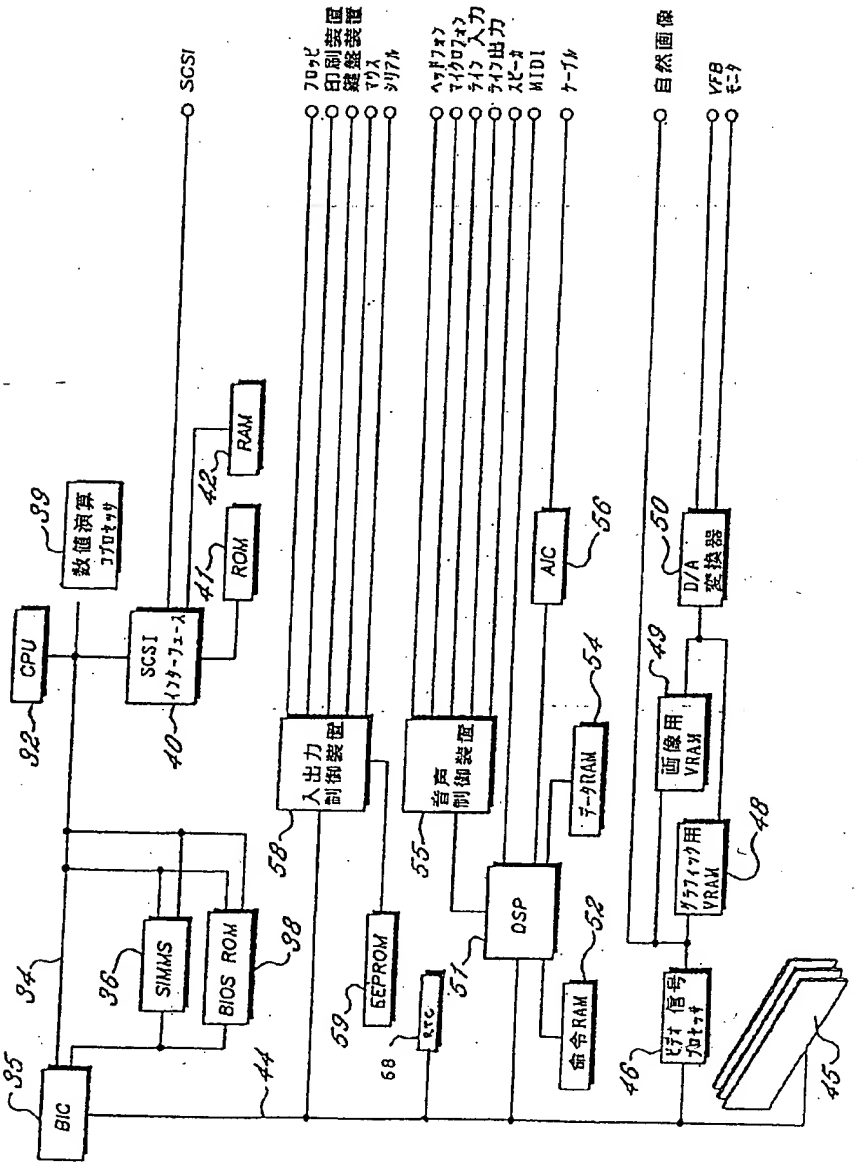
【図４】



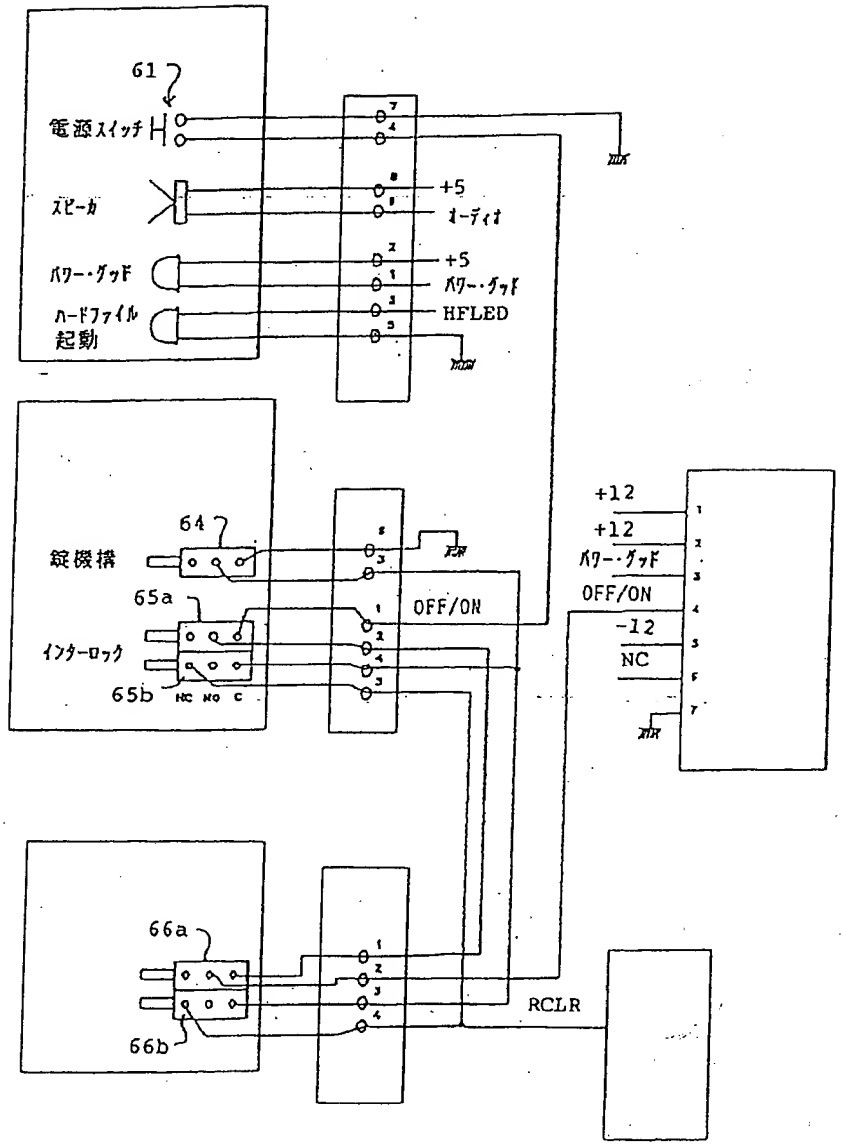
【図2】



【図3】


SCSI
フロッピ
印刷装置
鍵盤装置
マウス
ジョイスティック
ヘッドフォン
マイクロフォン
ライン入力
ライン出力
スピーカ
MIDI
ケーブル
自然画像
VTR
モニタ
数値演算プロセッサ
CPU
SCSIインターフェース
RAM
ROM
入出力制御装置
音声制御装置
AIC
D/A変換器
データRAM
画像用VRAM
グラフィック用VRAM
SIMMS
BIOS ROM
EEPROM
RTC
DSP
命令RAM
ビデオ信号プロセッサ
BIC

【図5】



フロントページの続き

(72)発明者　リチャード・アラン・ダヤン
アメリカ合衆国33487　フロリダ州ボカ・レイトン、エヌイー・73番ストリート　830
(72)発明者　デニス・リー・モエラー
アメリカ合衆国33487　フロリダ州ボカ・レイトン、ローズウッド・サークル　7430
(72)発明者　バルマー・ユージーン・ニューマン
アメリカ合衆国33433　フロリダ州ボカ・レイトン、ダブリン・ドライブ　7488
(72)発明者　ケネス・ジョン・ピーター・ズベイ
アメリカ合衆国33422　フロリダ州ボカ・レイトン、アイアンウェッジ・ドライブ　22845